TamPub This document has been downloaded from TamPub.uta.fi
The Institutional Repository of University of Tampere

© 2018 IMIA and Schattauer GmbH

Ethics Certification of Health Information Professionals

Eike-Henner Kluge[1], Paulette Lacroix[2], Pekka Ruotsalainen[3]
[1] Department of Philosophy, University of Victoria, Victoria, Canada
[2] PC Lacroix Consulting Inc., North Vancouver, Canada
[3] University of Tampere, School of Information Sciences, Tampere, Finland

Summary

Objectives: To provide a model for ensuring the ethical acceptability of the provisions that characterize the interjurisdictional use of eHealth, telemedicine, and associated modalities of health care delivery that are currently in place.

Methods: Following the approach initiated in their Global Protection of Health Data project within the Security in Health Information Systems (SiHIS) working group of the International Medical Informatics Association (IMIA), the authors analyze and evaluate relevant privacy and security approaches that are intended to stem the erosion of patients' trustworthiness in the handling of their sensitive information by health care and informatics professionals in the international context.

Results: The authors found that while the majority of guidelines and ethical codes essentially focus on the role and functioning of the institutions that use EHRs and information technologies, little if any attention has been paid to the qualifications of the health informatics professionals (HIPs) who actualize and operate information systems to deal with or address relevant ethical issues.

Conclusion: The apparent failure to address this matter indicates that the ethical qualification of HIPs remains an important security issue and that the Global Protection of Health Data project initiated by the SiHIS working group in 2015 should be expanded to develop into an internationally viable method of certification. An initial model to this effect is sketched and discussed.

Keywords

Ethics; health informatics professionals; certification

Yearb Med Inform 2018:37-40
http://dx.doi.org/10.1055/s-0038-1641196

CC BY-NC-ND 4.0

Introduction

Modern health care in all its forms, whether at the administrative or operations levels, increasingly relies on the development, implementation, and use of health care information systems and clinical data exchange between electronic health records (EHRs) over organisational and geographical jurisdictions. Increasingly, these complex socio-technical information systems are being outsourced to commercial service providers and use software as a service (SaaS) solutions, networked by the Cloud. The need to share sensitive health care information across jurisdictional borders brings with it challenging security, privacy, and ethical issues [1].

Security standards adopted by international organisations such as the Organisation for Economic Co-operation and Development (OECD) and the International Organisation for Standardisation (ISO) are widely used in the design and development of health care information systems. Privacy by Design is a model adopted by the privacy community as a process for software developers to design, develop, and implement information systems where privacy is the default [2-4].

While security standards and privacy practices may have a general ethical basis, they are typically focused on the technical development of systems and the management of data. What has been missing until recently in the development and management of health care information systems is an ethical code for health informatics professionals (HIPs) who are responsible for the governance, management, procurement, and security of health care information systems.

In 2015, the Security in Health Information Systems (SiHIS) working group of the International Medical Informatics Association (IMIA) initiated a long-term project, the Global Protection of Personal Health Data, to identify the requirements for protecting personal health information within an international context. The working group held workshops and collaborated with others in the field to identify appropriate security, privacy, and ethical measures for rectifying current issues.

The recently revised IMIA Code of Ethics for Health Information Professionals [5], that is based on the Universal Declaration of Human Rights (UDHR), has found general acceptance in the international community of informatics professionals. The UDHR, proclaimed internationally in 1948, explicitly mentions and indeed is based on several fundamental ethical principles that are recognized as binding on all persons, governments, and agencies irrespective of differences in socio-cultural or legal frameworks [6]. The IMIA Code encompasses these fundamental principles and provides a set of derivative principles and rules that are specific to health informaticians. The authors suggest that these can serve as the basis for a globally valid ethics-based certification programme for HIPs.

The term *certification* has many meanings. Certification can be a formal procedure or it can refer to the confirmation of certain characteristics of an object or entity. In this paper, the latter definition is used. For example, certification of HIPs would indicate that a health informatics professional would know, understand, and apply ethical principles in the governance, management, and operations of health care information systems and EHRs.

It is important to note that other professional organisations have also adopted ethical codes, standards, and guidelines for the development of health care information systems, software engineering, implementation and management of these systems, and the contents of the EHR. Organisations include, among others, the Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), Health Information and Management Systems Society (HIMSS), and the American Health Information Management Association (AHIMA).

Compared to these previous codes of ethics and guidelines, this paper presents a unique viewpoint that is focused on the fiduciary relationship that exists between HIPs, health care professionals, and the subject of care (the patient), and how HIPs act ethically in this relationship.

Method

As a preamble to its constructive work, the authors conducted a review of privacy principles and security standards in order to determine what had and what had not been done, and in what sense ethical considerations had been integrated into the various undertakings. The authors found that privacy and security was the subject of considerable attention, relative to the recent General Data Protection Regulations of the European Union (GDPR) [7], but most importantly it appeared that trustworthiness figured largely as an underlying theme in a series of official and regulatory pronouncements. The authors also found attempts to place trustworthiness in a measurable footing using system modelling methods, system analysis, and system engineering techniques [8].

The authors also evaluated privacy, security, and trust approaches with respect to their ethical soundness and interjurisdictional usability in light of the existing differences in professional and legal standards. Based on these findings the authors developed a proposal for an international ethics-based HIP certification programme.

Results

Existing Guidelines and Codes of Conduct

The authors found that while the majority of guidelines and ethical codes essentially focused on the role and functioning of the institutions that use EHRs, information technologies themselves, and on what had been developed to maintain system security and functionality, there was also recognition that these codes should extend to HIPs who actualize and operate the systems. The authors therefore investigated what measures of qualification had been developed for HIPs, and also what certification and education programmes had been developed for them [9-14]. These findings were further subjected to a similar analysis relative to their ethical tenability, situational appropriateness, and interjurisdictional validity.

In the main, the authors found that at the institutional, corporate, and vendor levels the focus of ethical codes and guidelines were centred in security, confidentiality, usability, and technology as well as in the ability to respond quickly to specific needs as these arise in the various contexts. It also became apparent that existing ethical codes and guidelines were neither integrated nor mutually consistent, and there was no attempt made by the institutions, corporations, or vendors to validate their ethical acceptability.

As to codes of conduct for HIPs, it was found that they tended to conflate ethical and legal considerations. Actually, there were some exceptions. For instance, the American Medical Informatics Association has developed a code of conduct for its members and has even promulgated guidelines for the secondary use and re-use of health care data [15-17]. The British Computing Society has also developed a code of conduct [18], as had the Australasian College of Health Informatics [19]. Another example came from Canada, where Digital Health Canada has promulgated a set of core competencies [20] which, to some degree, contained ethical considerations.

However, the primary focus of all such codes, documents, and provisions was not global in health care system orientation, and was only focused on eHealth, telemedicine and related modalities. As well, the codes and other provisions were not integrated with other ethical codes and guidelines that should be adhered to by health care organisations. The application of these codes and provisions tended to focus on considerations that were relevant to the respective jurisdictions in which they were developed, and hence they were of limited use in the international setting. It appeared that there was no evaluation of ethical proficiency, and the authors found that current HIP certification programmes were not global in scope.

HIP Certification Programme

The purpose of certification is to ensure appropriate ethical knowledge is adhered to by HIPs and the health care organisations in which they operate. As the IMIA Code of Ethics indicates, the ethics of health informatics deals with the actions of HIPs who are involved in the collection, use, security, appropriate disclosure, retention, and disposition of data in the domain of health care. This means that being certified in health information ethics testifies that whoever is thus certified is familiar with and proficient in the ethical aspects of several distinct areas. These include specific topics in health information ethics with which candidates should be familiar as well as what might be called the vector space of the rights and duties that are involved in these areas. These are outlined in the IMIA Code of Ethics.

The certification process should be applied to include all HIPs that are working in health care organisations, whether public and private. Certification would not only establish their ethical proficiency as professionals but would also be consistent with the general tenor of the European GDPR and related provisions.

The most effective format for measuring certification proficiency for HIPs would be by means of a standardized test. The test would rely on scenarios that involve the issues in which proficiency is sought and would consist in having candidates correctly identify the ethical issues involved, the parties who are affected, determine whether the issues have been handled ethically appropriately, and have the candidates suggest what should have been done if they have not been handled correctly. The particular areas and subjects presented in these scenarios would follow the headings that are identified

as ethically important in the IMIA Code of Ethics. The scenarios would illustrate multiple issues as these occur in real life, and the answer sections would consist of a mix of true-false and multiple-choice options. The scenarios would be based on actual cases that have proved problematic, where of course care would be taken to alter identifying details so that the privacy of the relevant parties would be protected.

The test itself would be in the nature of a secure on-line interactive web page, and there would be a time limit for completing the task. This format would allow candidates to access reference materials when answering the questions. However, rather than being a shortcoming, this would be in keeping with real life. An ethically sensitive and trained individual could, when in doubt, consult relevant and appropriate reference material.

The certification could be handled and administered by a specified international organisation with ethics expertise to function as authority. For instance, IMIA in cooperation with an appropriate body of the World Health Organisation (WHO) has the requisite expertise and could function as a certifier. This option would have the advantage of drawing on international professional health informatics expertise as well as the health-related expertise of the WHO in the context of current eHealth and telemedicine developments, and would ensure that industrial and commercial interests would not supersede ethical considerations.

Unquestionably, there would be costs associated with developing, implementing, and administering the certification programme. It is important to present certification itself as not being subject to proprietary and fiscal interests that might influence the quality or neutrality of the process itself.

The very nature of ethical certification is to ensure that appropriate ethical knowledge and understanding is adhered to by HIPs and the organisations in which they work, and that the ethical treatment of EHRs that underlies the reason for certification in the first instance is not subject to non-ethical considerations.

Discussion

The Universal Declaration of Human Rights and the IMIA Code of Ethics for Health Information Professionals form the basis of an ethics-based certification programme for HIPs proposed by the authors. The aim of the certification solution proposed here is to ensure that appropriate ethical knowledge and understanding is adhered to by HIPs. To engage in professional and technical activities without having the appropriate ethical competence amounts to a violation of the Principle of Fidelity and constitutes malfeasance of duty [21]. Technical proficiency is no guarantee that anyone would use the knowledge, products, or services that are at his/her disposal in an ethically appropriate manner. If it were otherwise, for example if the technical competence were all that was necessary for proper professional activity, there would be no need for ethical standards and codes of ethics, and there would never be any need for professional disciplinary procedures. Ethical proficiency, therefore, should be integral to professionalism, and the proposed certification solution is intended to certify such proficiency in a measurable sense.

From the other side, it is evident that knowing ethics rules is not enough. HIPs have also to behave ethically in real life situations. While it is technically possible to monitor behaviours of HIPs, this is not generally accepted and can be a violation of privacy rights. To act ethically inside of a health care organisation, there should be minimal to no conflicts between the organisational ethics and the ethical code of a certified HIP. Despite the availability of general ethics university courses and training programs, the authors suggest that the role of a HIP in a health care setting is so unique that a health care related ethics-based certification is needed. A meaningful challenge is that in many countries the professional designation of HIPs does not exist. As health information systems are outsourced, it may be difficult to determine which persons would require the proposed certification.

A big question is how effective the proposed HIP certification would remedy the issues with hardware and software used in health information systems, namely the trustworthiness of the system and EHR. If an ethical lense is applied to the design, development, implementation, governance, and ongoing maintenance of a health information system, would accountability in the use and disclosure of health care information in the EHR improve the overall usability and security of the system ? The authors believe that the ethics certification of HIPs is a realistic step, with further extension of a vision that can only be true with large scale international regulators and multi-faceted cooperation. A less desirable outcome is the eroding trustworthiness of health information systems by the health care public where a digital system that purports beneficial outcomes lacks ethical oversight, and breaches of sensitive health information become the new normal.

The desirability of national certification for HIPs in technical matters appears to be well established and, as was already indicated, various national health information organisations either have developed or are in the process of developing certification programmes that would meet the technical standards set out by the ISO/TC 215 Health Informatics [22]. At the same time, the development of ethically-based certification provisions at a national level would not address the issue of interjurisdictional ethical validity. This may present logical and conceptual difficulties when trying to develop globally defensible rules for ethical certification.

To illustrate this point, a significant proportion of ethically unfortunate (or questionable) events that involve EHRs in outsourcing is due to a lack of clarity of what the relevant standards are and how they should be applied when national boundaries are crossed. Thus, it is currently unclear how the ethical codes and/or principles that prevail in one jurisdiction should be applied. Even more importantly, what fundamental principles should be used when health information services are outsourced from one jurisdiction to another [23]. For example, it is unclear what standards, ethics, or principles should apply when radiographs originating from Chicago are read in Bangalore or Zurich, when health service related billings originating from Berlin or Mexico City are outsourced to Bloomington, Indiana, or Chennai [24-28], or when medical notes that have been taken in one country are outsourced for transcription in EHRs to other countries where not only professional standards are different but even the native language of the transcribing individuals is other than that of the note-taking medical professionals [29]. What ethical considerations, if any, are relevant, and in what sense ?

At first glance, this state of affairs presents insurmountable practical difficulties. Arguably, it would be impossible to establish a HIP ethics certification programme in general that has global validity unless it was possible to identify ethical principles that are recognized as being universally valid. More particularly, it would seem impossible to develop an informatics ethics certification programme unless there was a generally accepted set of ethical principles and rules specific to health informatics that could form its basis. This step has already been taken with the development of the IMIA Code of Ethics for Health Information Professionals. What remains to be done is to use this Code as a foundation and, with the effective involvement of relevant global bodies such as the WHO and IMIA, to develop a certification programme that has international validity.

Conclusion

The ethics-based certification of HIPs is a desideratum that currently is not being met, whether that be at national levels or in the wider international context. The issue of accountability in the design, development, and implementation of health care information systems and the intra-jurisdictional transfer of information become ever more important as EHRs continue to supersede paper-based records and as eHealth, telemedicine, and related modes of health care delivery using EHRs continue to develop. The need becomes positively pressing as EHR-related services are outsourced to information technology providers who are not themselves engaged in the delivery of health care but merely provide an informatics service, and because the framework of fiduciary obligation that binds health care providers does not exist in their case. The certification programme proposed by the authors is intended to meet this important need.

References

1. Ruotsalainen P, Blobel B. Trust Model for protection of personal health data in a global environment, in the Proceedings of MEDINFO 2017, August 21-25, 2017, Hangzhou, China. Stud Health Technol Inform 2017;245:202-6.
2. Organisation for Economic Co-Operation and Development. The OECD Privacy Framework. OECD Publishing; 2013. Available from: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [Accessed: 26 February 2018].
3. International Organisation for Standardisation. Available from: https://www.iso.org/home.html [Accessed: 26 February 2018].
4. Cavoukian A. Privacy by Design…Take the Challenge. Information and Privacy Commissioner of Ontario. Canada; 2009.
5. The IMIA Code of Ethics for Health Information Professionals. Available from: http://www.imia-medinfo.org/new2/pubdocs/Ethics_Eng.pdf [Accessed: February 26th 2018].
6. Universal Declaration of Human Rights. Available from: http://www.un.org/en/universal-declaration-human-rights [Accessed:February 26th 2018].
7. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en [Accessed:February 26th 2018].
8. Fong EN, Cleraux C, Boland Jr. FE. Toward a preliminary framework for assessing the trustworthiness of software. NIST Interagency/Internal Report (NISTIR). September 2010. Available from: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=906717 [Accessed: February 26th 2018].
9. National Institutes of Health. NIH Ethics Program. Training modules for staff: government employees and non-employees. Available from: https://ethics.od.nih.gov/training.htm [Accessed: February 26th 2018].
10. Compliance Certification. Certified compliance & ethics professional handbook. Available from: http://www.compliancecertification.org/Portals/2/PDF/CCEP/ccb-ccep-handbook.pdf [Accessed: February 26th 2018].
11. American Medical Informatics Association. Advanced health informatics certification. Available from: https://www.amia.org/ahic [Accessed: February 26th 2018].
12. Gadd CS, Williamson JJ, Steen EB, Fridsma DB. Creating advanced health informatics certification. J Am Med Inform Assoc 2016;23(4):848-50.
13. University of California, Davis Extension. Health informatics certificate program. Available from: https://extension.ucdavis.edu/certificate-program/health-informatics-certificate-program [Accessed: February 26th 2018].
14. Digital Health Canada. CPHIMS Certification. Available from: http://digitalhealthcanada.com/achieving-cphims-ca/ [Accessed: February 26th 2018].
15. American Medical Informatics Association: Code of professional and ethical conduct. Available from: https://academic.oup.com/jamia/article/20/1/141/728741 [Accessed: February 26th 2018].
16. Roberts A. Language, structure, and reuse in the electronic health record. AMA J Ethics 2017;19(3):281-8. Available from: http://journalofethics.ama-assn.org/2017/03/stas1-1703.html [Accessed: February 26th 2018].
17. American Medical Informatics Association. Secondary use and re-use of health care data: Taxonomy for policy planning and formulation. Available from: https://www.amia.org/sites/amia.org/files/2007-Policy-Meeting-amia-taxonomy-Secondary-Data-Use-Version.pdf [Accessed: February 26th 2018].
18. British Computer Society. BCS code of conduct. Available from: http://www.bcs.org/category/6030. [Accessed: February 26th 2018].
19. Australasian College of Health Informatics. Professional code of conduct. Available from: http://www.achi.org.au/docs/ACHI_Professional_Code_of_Conduct.pdf. [Accessed: February 26th 2018].
20. COACH: Canada's Health Informatics Association. Core Competencies. Available from: https://www.coachorg.com/en/resourcecentre/resources/Health-Informatics-Core-Competencies.pdf [Accessed: February 26th 2018].
21. Byrd GD, Winkelstein PA. Comparative analysis of moral principles and behavioral norms in eight ethical codes relevant to health sciences librarianship, medical informatics, and the health professions. J Med Libr Assoc 2014 Oct;102(4):247–56. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4188052/ [Accessed: February 26th 2018].
22. International Standards Organisation. Health informatics. ISO/TC 215. Available from: https://www.iso.org/committee/54960.html [Accessed: February 26th 2018].
23. Rohde, FH. IS/IT outsourcing practices of small- and medium-sized manufacturers. International Journal of Accounting Information Systems 2004;5(4):429–51. Available from: https://www.sciencedirect.com/science/article/pii/S1467089504000466 [Accessed: 26th February 2018].
24. Kalyanpur A, Neklesa VP, Pham DT, Forman HP, Stein ST, Brink JA. Implementation of an international teleradiology staffing model. Radiology 2004;232(2):415-9. Available from: http://pubs.rsna.org/doi/abs/10.1148/radiol.2322021555?journalCode=radiology [Accessed: February 26th 2018].
25. Steinbrook R. The age of teleradiology. N Engl J Med (2007);357:5-7.
26. Outsource Management Group. Billing Outsourcing Services for Medical Providers. Available from: http://www.outsourcemedicalbilling.com [Accessed: February 26th 2018].
27. Outsource2India. Outsource teletradiology services. Available from: https://www.outsource2india.com/services/teleradiology.asp [Accessed: February 26th 2018].
28. Burute N, Jankharia B. Teleradiology: The Indian perspective. Indian J Radiol Imaging. 2009 Feb;19(1):16–8. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2747412/ [Accessed: February 26th 2018].
29. Outsource2India. Medical Transcription Services. Available from: https://www.outsource2india.com/services/medical_transcription.asp [Accessed: February 26th 2018].

Correspondence to:
Eike-Henner Kluge
Professor
University of Victoria
3800 Finnerty Rd
Victoria, BC V8P 5C2, Canada
E-mail: ekluge@uvic.ca